



Metropolitan Nashville Public Schools recognizes that the effective use of electronic media and telecommunications networks enhance the quality and delivery of education in our schools by providing access to unique resources and opportunities for collaborative work.

MNPS supports the use of electronic communications for both students and employees and expects that all faculty and staff will thoroughly integrate the use of voice, data and video technologies throughout the school system and in the teaching and learning process, including educational social networking sites with proper monitoring and appropriate permissions.

However, the use of electronic technology is a privilege and is subject to all applicable state and federal laws and policies of the district. MNPS reserves the right to examine electronic mail messages, files on all types of MNPS computers and servers, web browsers, cache files, websites, website logs and any other information stored or passing through our information systems. Parents will be required to sign an Acceptable Use Agreement, which will be kept on file at each school, for student who wishes to access the MNPS network. Employees must sign an Acceptable Use Agreement as well which will be kept on file.

At no time shall there be an expectation of privacy by employees of students while utilizing any MNPS network or stand-alone system. The district reserves the right to examine any information originating on, accessed by or processed through MNPS owned computers, networks or other information system components. This examination may occur with or without the user's prior knowledge and may be conducted in real time or by examining access history and/or related files. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed and/or stored by others. Electronic communications are also retrievable after the user has deleted them from his/her system, so it is best practice not to store personal confidential information on a district machine or server.

Date Published
October, 2008

Revision History

Review
Annually

Acceptable Use of Electronic Media and Telecommunications Networks

IM 4.153

In accordance with federal law, MNPS shall ensure the safety of students through strict enforcement of acceptable use guidelines and a filtered network that is consistently monitored for unacceptable content pursuant to 47 USC §254(h) and the Children's Internet Protection Act (CIPA).

All users (students and employees) shall comply with the following when accessing the internet or using e-mail on the MNPS network:

- The MNPS network may only be used for educational and professional purposes, consistent with the mission and goals of the district. Commercial use of the MNPS network is strictly prohibited.
- Accessing or transmission of threatening, offensive or harassing information (text or images) which contains defamatory, abusive, obscene, pornographic, profane, sexually oriented, racially offensive, or otherwise biased, discriminatory or illegal materials shall be strictly prohibited.
- Users may access copyrighted material for research purposes, but its use must strictly adhere to the agreement posted by the author and/or current copyright law (17 USC §101).
- Transmission of incendiary statements that potentially might incite violence or describe or promote the use of weapons or devices associated with terrorist activities shall be strictly prohibited.
- Attempting to subvert network security, impair the functionality of the network, or to bypass restrictions set by network administrators is forbidden. This includes creation and use of proxy servers.
- Users are assigned specific usernames and passwords in order to conduct business on the MNPS network. These passwords are not to be shared with anyone. If a breach is discovered, the user must contact the MNPS helpdesk to change their password as quickly as possible after the discovery.
- Use of "system" or "administrative" passwords is prohibited by unauthorized individuals.
- Downloading copyrighted music, video recordings, or unapproved or illegal software onto the MNPS network is prohibited.
- The distribution of chain letters, spam, advertisements and unauthorized solicitations is unacceptable and forbidden.
- Unauthorized access, including "hacking" is prohibited. Unauthorized tampering with, or access to, the district's student management system that results in changes to student information is unlawful and a violation of the Family Educational Rights and Privacy Act (FERPA, 34 CFR Part 99).
- Students will be instructed in proper use of internet and e-mail by the appropriate school personnel and will be monitored while utilizing district computers.
- Contractors and consultants who have been granted temporary access to the MNPS network shall be governed by the same policy, rules and regulations as students and employees. Additional restrictions may be imposed when access is given to confidential information.

Monitoring and Reporting Alleged Policy Violations

System administrators will not routinely monitor user internet and e-mail activities and will take reasonable precautions to protect user privacy. However, MNPS may monitor a user's internet and/or e-mail activity when there is a legitimate business or technical need to do so. Circumstances that would warrant this level of access or monitoring include, but are not limited to:

- When there is a need to access information when a user is absent for an extended period of time or unavailable to assist technical personnel
- When there is a need to diagnose and/or resolve technical problems involving system hardware, software or communications
- As an incidental activity when conducting network maintenance
- When there is a need to gather information required for litigation
- As a part of testing performed by auditors
- When a reasonable suspicion exists that a user is engaging in unprofessional and/or illegal activities that are facilitated by or otherwise involve use of the MNPS network
- As a part of an investigation of a possible crime or violation of MNPS policy
- When there is a legal requirement to disclose e-mail or internet activity to law enforcement officials
- When there is a request for access to information under the Open Records Act

Alleged violations involving student use shall be reported to the teacher who was supervising the student at the time of the alleged offense. The teacher or staff person shall report the alleged violation to the principal, who will investigate the incident, with appropriate input from the Information Technology department. If after the investigation there is a reasonable certainty that a violation actually occurred, the principal will impose sanctions, which may include limiting or suspending a student's internet privileges. Serious or repeated violations of internet or e-mail use could result in permanent loss of internet and/or e-mail privileges, and other disciplinary action consistent with the Student Code of Conduct. If a student's misuse of internet or e-mail is in violation of the law, such misuse shall be reported to the appropriate authorities and could be punished as a criminal offense.

Alleged violations involving employees shall be reported to the appropriate principal or department head, who will investigate the incident with input from the Information Technology Department. Clear and willful violations or abuse of acceptable usage as set forth in this policy will be subject to disciplinary actions, depending on the severity of the transgression and policy abuse, up to and including termination. Criminal or civil action may be initiated if the violation involves action that is against the law.

Disclaimer of Liability

- MNPS makes no warranties of any kind, either express or implied, that the functions or the services provided by, or through, the MNPS network will be error-free or without defect. MNPS will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruption of services.

Acceptable Use of Electronic Media and Telecommunications Networks

IM 4.153

- MNPS is not responsible for the content of any advice or information received by a user from a source outside MNPS, or any costs incurred as a result of such advice. MNPS will make every reasonable effort to supervise students' internet and email use, but will not be responsible for claims and liabilities arising from such use.
- MNPS will not be responsible for financial obligations incurred or arising through the use of the system by employees.
- MNPS is not responsible for the communications of individuals utilizing the MNPS network.
- Parents will be held financially responsible for any harm to the system as a result of a student's intentional and malicious misuse.

References/Authority

Children's Internet Protection Act (CIPA) 47 USC §254(h)(1)

Family Educational Rights and Privacy Act (FERPA) 20 USCA §1232(G)

TCA §10-7-512

TCA §39-14-602

TCA §39-4-105

17 USCA §107

17 USCA §117